CITY OF SAN ANTONIO

Administrative Directive	**AD 7.8.1 Information Security Program**
Procedural Guidelines	Policy, procedures, and controls of a security program to protect City of San Antonio information assets.
Department/Division	Information Technology Services Department (ITSD)
Effective Date	May 14, 2010
Project Manager	ITSD

Purpose

The purpose of this Administrative Directive (AD) is to define and implement procedures and controls at all levels to protect the confidentiality, integrity, and availability of City information assets.

Policy

All City information assets must be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction – whether accidental or intentional – in order to maintain their confidentiality, integrity, and availability. Access to all City, non-public, information assets will be limited to what is necessary for the performance of required tasks.

Information security is a responsibility shared by senior City officials, all City managers and staff, system owners, information technology (IT) professionals, and all other users of City information assets. The City's information security program shall provide policies, standards, procedures, and guidelines to ensure the protection of our information assets.

Policy Applies To

☐ External & Internal Applicants	☒ Current Temporary Employees
☒ Current Full-Time Employees	☒ Current Volunteers
☒ Current Part-Time Employees	☒ Current Grant-Funded Employees
☒ Current Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Current Contract Employees

Definitions	
Accreditation	Authorization by the Information Technology Services Department (ITSD) Chief Technology Officer (CTO), or designee, to place an information asset into operation.
Availability	Ensuring that information assets, including stored information and processing capability, are always available to authorized users when needed.
Certification	The technical and non-technical evaluation of an information asset – by the system owner or by an independent certifying agent – that produces the necessary information required by an authorizing official to make a credible, risk-based decision on whether to place an information asset into operation.
Confidentiality	Ensuring that the information and processing capabilities of City information assets are protected from unauthorized disclosure or use.
Controls	The means of managing risk, which includes policies, procedures, guidelines, practices, or organizational structures. Controls may be management (e.g., risk management plan), operational (e.g., strong password rules), or technical (e.g., corporate firewalls) in nature.
Corrective Actions	Steps that are taken to address existing nonconformities and make improvements. Corrective actions deal with actual nonconformities (problems), ones that have already occurred. They solve existing problems by removing their causes. In general, the corrective action process can be thought of as a problem solving process.
Information Asset	All records, documents, data, and systems created, owned, or managed by the City.
Information Security	Measures taken to preserve the confidentiality, integrity and availability of information assets; ensures that information is authentic, reliable, and from an accountable source.
Information Systems	Computers, hardware, software, storage media, and networks; the procedures and processes used to collect, process, store, share or distribute information by and through the City's computing and network infrastructure.
Integrity	Ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.

Preventive Actions	Steps to prevent the occurrence of problems by removing their causes or reduce the likelihood that they will occur. In general, the preventive action process can be thought of as a risk management process.
Risk	The possibility that an event will adversely impact the City's information assets. The potential risk is measured by the cost of the risk to the City, if realized, discounted by the probability, or the likelihood, that the risk will occur.
Risk Assessment	A process to identify, analyze, and manage potential risks.

Policy Guidelines

General Guidelines

SCOPE

A. This directive applies to all management, users, system owners/managers, system maintainers, system developers, operators, and administrators, including vendors, contractors, and third parties, of City information assets, facilities, and communications.

B. This directive applies to all information collected or maintained by or on behalf of the City and all information assets used or operated by the City, a City contractor, a City vendor, or any organization on behalf of the City.

PROGRAM

C. A citywide information security program will help protect City information assets from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction – whether accidental or intentional – in order to maintain their confidentiality, integrity, and availability.

D. The information security program defines the management, operational, and technical controls necessary to protect City information assets, in accordance with the risks that threaten such assets.

E. The information security program is based on five elements:

1. *Information Security Asset Classification* – protects City information assets through the implementation of asset classification and controls; ensures that City information assets are identified, properly classified, and protected throughout their lifecycles.
2. *Information Security Management Controls* – protects City information assets through the implementation of management controls that define the required behavior expected by those in leadership positions in the City.
3. *Information Security Operational Controls* – protects City information assets through the implementation of operational

controls that define the required behavior expected by City employees and those given access to the City's information assets.

4. *Information Security Technical Controls* – protects City information assets through the implementation of technical controls that reduce the exposure of computer equipment and assist in achieving an optimum level of protection for the City's information assets.

5. *Information Asset Certification and Accreditation* – ensures that information assets are authorized to function in an operational environment under defined and acceptable information security controls.

F. ITSD shall define and publish policies and guidelines, such as business procedures and information security plan templates, to direct departments and users as they implement these practices and controls. ITSD shall work with information asset owners to establish implementation timelines.

G. Based upon templates established by ITSD, each department is required to establish information security plans that conform to the enterprise information security program and protect all information assets under departmental control. Each department information security plan needs to include preventative, detective, and corrective controls to provide a reasonable level of information security. Each plan needs to:

1. Assign development and management responsibilities for information security, including the designation of an executive-level information security liaison.

2. Provide for the confidentiality, integrity, and availability of information assets under departmental control.

3. Assess the potential risk impact to City information assets, including the cost if the risk is realized, and help implement risk management measures.

4. Participate in the creation, testing, and maintenance of enterprise and departmental incident response plans.

5. Coordinate the delivery of security awareness and training programs.

H. Information security roles and responsibilities must be identified and defined to achieve security objectives and manage risk throughout the City. Each department must define the functions, relationships, responsibilities, and authorities of individuals or groups that support the information security program.

RISK MANAGEMENT

I. Risks to information assets must be actively managed in order to prioritize resources and remediation efforts. Risk management

	involves the identification and evaluation of risks to information assets (risk assessment) and the development of strategies to manage those risks. Examples of information security risks include criminal attacks, theft of equipment, malware or viruses, and natural disasters. J. Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. COMPLIANCE K. Each department, in consultation with the City Attorney's legal staff and other subject matter experts, must regularly identify the laws and regulations that apply to City information assets. The information security policies and standards must comply with applicable federal, state, and municipal laws, regulations, court orders, and contractual obligations that apply to City information assets. ENFORCEMENT L. The City can temporarily or permanently suspend, block, or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of City resources, to protect the City from liability, or to comply with applicable federal, state, and municipal laws, regulations, court orders, and contractual obligations.
Roles & Responsibilities	
Chief Information Officer (CIO)	A. Ensures that a citywide information security program exists, that it complies with federal, state, and municipal laws, regulations, court orders, and contractual obligations that apply to City information assets and it is being followed. B. Ensures that information security management processes are integrated with the City strategic and operational planning processes.
Chief Technology Officer (CTO)	A. Oversees implementation and administration of the City information security program. B. Oversees the integration of security management processes into departmental strategic and operation business processes.
Information Technology Services Department (ITSD)	A. Develops and implements, with input from City leadership and system owners, additional policies, standards, guidelines and procedures that fully comply with all City directives. B. Carries out information security responsibilities, including: 1. Develops and maintains the citywide information security program;

	2. Develops and maintains information security policies, guidelines, and control techniques to address all applicable requirements; 3. Trains and oversees personnel with significant responsibilities for information security; and 4. Assists senior City officials as well as system owners in understanding their security responsibilities. C. Ensures the scheduled execution (based upon a frequency set by policies and guidelines) of: 1. Periodic risk assessments; 2. Certification and accreditation of all information systems including annual security testing and security self assessments; 3. Development, testing, and updating of contingency plans; and 4. Providing security and awareness training to all employees and specialized (role-based) training to those with significant security responsibilities. D. Publishes and maintains these policies, standards, and guidelines in a City information security handbook.
Departments	A. Appoint an executive-level liaison to manage and coordinate the information security responsibilities of the department. B. Assess the risks and potential magnitude of harm to the information assets over which they have control that could result from the unauthorized access, use, disclosure, disruption, duplication, modification, diversion, or destruction – whether accidental or intentional – of City information or information systems that support the operations and assets of the department. C. Follow security directives, policies, and guidelines. D. For those information assets under the department's control: 1. Create plans for providing adequate information security. 2. Coordinate annual information security awareness training for departmental personnel, including contractors and other users of information assets under departmental control. 3. Test and evaluate, including self-assessments, the effectiveness of the information security plans, policies, and guidelines with a frequency depending on risk, but no less than annually. 4. Plan, document, and evaluate remedial actions to address any deficiencies in the implementation of the information security plans, policies, and guidelines. 5. Maintain certification and accreditation for all information assets including updating security plans and risk assessments; develop processes for detecting, reporting, and responding to security

	incidents for information assets within the department's control.
Employees and Users	A. Ensure the protection of City information assets from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction – whether accidental or intentional – by complying with the information security requirements maintained in City directives, policies, and guidelines.
Attachments	
N/A	

Information and/or clarification may be obtained by contacting the Information Technology Services Department (ITSD) at 207-8301.

CITY OF SAN ANTONIO

EMPLOYEE ACKNOWLEDGMENT FORM
FOR

ADMINISTRATIVE DIRECTIVE 7.8.1

Information Security Program

Effective TBD

Employee:

I acknowledge that on _____, 20__, I received a copy of Administrative Directive 7.8.1, Information Security Program.

_____ _____

Employee Name (Print) Department

_____ _____

Employee Signature SAP Employee ID Number

Supervisor:

I certify that on _____, 20__, I provided a copy of this administrative directive to the above named employee.

_____ _____

Supervisor (Print) **Supervisor Signature**

HR / AD
(As of 2009)

201 File (original)
Field Folder Copy
Employee Copy